UNITED STATES DISTRICT COURT
DISTRICT OF MASSACHUSETTS

AUDREY ARPIE, on behalf of herself and all others similarly situated, Plaintiffs, vs. UKG, INC., MERCY MEDICAL GROUP, INC., and TRINITY HEALTH OF NEW ENGLAND CORPORATION, INC. Defendants.	Case No. _____ **CLASS ACTION COMPLAINT** **JURY TRIAL DEMANDED**

Plaintiff Audrey Arpie ("Ms. Arpie" or "Plaintiff") on behalf of herself and all others similarly situated (the "Class" or "Class Members"), brings this action against Defendants UKG, Inc. ("UKG"), Mercy Medical Group, Inc., and Trinity Health of New England Corporation, Inc. (collectively, the "Defendants") to obtain damages, restitution, and injunctive relief for the Class. Plaintiff alleges the following based on personal knowledge, the investigation of counsel, and information and belief.

NATURE OF THE ACTION

1. Plaintiff and Class Members are hourly employees who were not paid the full amount of wages to which they are entitled for all of their work in a timely fashion by Defendants.

2. Plaintiff and Class Members provided their personally identifiable information ("PII") to Defendants at their request, including names, addresses, employee IDs, and social security numbers. Due to Defendants' failure to implement and maintain reasonable safeguards to protect Plaintiff's PII, criminals obtained access to Plaintiff's PII, which resulted in substantial

harm to Plaintiffs and the Class.[1]

3. This class action seeks to redress Defendants' unlawful withholding of wages for Plaintiff and Class Members and the negligent disclosure of over 8 million employees' PII in a massive data breach on or around December 11, 2021 ("Data Breach"). On that date, and possibly on others, Defendants' inadequate security measures allowed unauthorized individuals to access and render unusable a workforce management software application Defendants used to process payroll and store data that contained the PII of Plaintiff and other individuals.[2]

4. As a result of the Data Breach, Plaintiff and Class Members were not timely paid the full amount of wages to which they are entitled.

5. Plaintiff and the Class Members also now bear an immediate and heightened risk of all manners of identity theft. Plaintiff has incurred, and will continue to incur, damages in the form of, *inter alia*, an imminent threat of identity theft, loss of privacy and the value of personal information, deprivation of the benefit of the bargain, and/or the additional damages set forth in detail below.

JURISDICTION AND VENUE

6. This Court has personal jurisdiction over Defendant Mercy Medical Group, Inc., because it maintains a headquarters in and has its principal place of business in Massachusetts.

7. This Court has personal jurisdiction over Defendant Trinity Health of New England Corporation, Inc. because it has had systematic and continuous contacts with the State of Massachusetts. Trinity Health is registered to do business in Massachusetts with the Massachusetts Secretary of State. Trinity Health, through its operation of Mercy Medical Group,

[1] *See UKG Kronos Community*, Communications Sent to Impact Kronos Private Cloud (KPC) Customers, https://community.kronos.com/s/feed/0D54M00004wJKHiSAO?language=en_US.
[2] *See id.*

Inc., and its affiliated hospitals within Massachusetts, operates integrated health care delivery systems within Massachusetts.

8. This Court has personal jurisdiction over Defendant UKG Inc. because it has had systematic and continuous contacts with the State of Massachusetts. UKG is registered to do business in Massachusetts with the Massachusetts Secretary of State. UKG contracts with many businesses in Massachusetts to provide human resources services, including payroll services.

9. This Court has jurisdiction over this action under the Class Action Fairness Act ("CAFA"), 28 U.S.C. § 1332(d), because the aggregate amount in controversy exceeds $5,000,000, exclusive of interests and costs, there are more than 100 class members, and Plaintiff and one or more members of the classes are residents of a different state from a defendant.

10. This Court has jurisdiction over the Massachusetts Wage Act claim pursuant to M.G.L c. 149, § 150, as well as the federal supplemental jurisdiction statute 28 U.S.C. § 1367(a).

11. Venue is proper in the District of Massachusetts because, pursuant to 28 U.S.C. § 1391(b)(2) in that a substantial part of the events or omissions giving rise to the claims occurred in Massachusetts.

PARTIES

12. Plaintiff Audrey Arpie is a citizen of Massachusetts and a resident of Agawam, Massachusetts.

13. On approximately December 11, 2021, Plaintiff's PII was exposed in the Data Breach. On one or more weeks after December 11, 2021, Plaintiff was not timely paid for the full amount of wages due and her PII was exposed. If Plaintiff had known that Defendants would not adequately protect her PII, she would have either refused to provide such information, or taken action to challenge the condition of employment imposed by Defendant Mercy Medical Group,

Inc. and Trinity Health of New England Corporation, Inc. ("Mercy") that she disclose PII and prohibit Defendants' access to this sensitive and private information until the Data Breach security issue was resolved.

14. Defendant Mercy Medical Group, Inc. is a Massachusetts Nonprofit Corporation with its principal place of business at 271 Carew St., Springfield, MA 01104.

15. Defendant Trinity Health of New England Corporation, Inc. is a Connecticut Corporation with its principal place of business at 114 Woodland St., Hartford, CT 06105.

16. Defendant UKG Inc. is a Delaware Corporation with its principal place of business at 2000 Ultimate Way, Weston, FL 33326.

FACTUAL BACKGROUND

A. Plaintiff's Status As An Employee

17. Plaintiff was employed by Mercy as an hourly employee during the relevant time period.

18. During the relevant time period, Mercy employed hourly employees to work in numerous sectors of the health care industry.

19. Plaintiff's principal job duties included, but were not limited to, providing care for Mercy's patients as a registered nurse.

20. Plaintiff was paid on an hourly basis.

21. Mercy regularly scheduled Plaintiff's work hours.

22. Plaintiff regularly reported her hours to Mercy, as instructed by Mercy.

23. Mercy regularly received reports indicating the hours worked by Plaintiff.

24. On or about December 13, 2021, Mercy instituted a "payment freeze" for all hourly employees, such that the pay for each pay period following that date was set arbitrarily to the

period prior to the freeze, with limited exception.

25. Mercy failed to pay Plaintiff the full amount of wages to which she was entitled for all of her work time in a timely fashion.

26. Plaintiff or Plaintiff's representative made numerous requests for payment of their wages in full, but these requests were denied.

27. Plaintiff did not furnish her work gratuitously.

28. Plaintiff worked with the expectation that she would be paid in full for all hours worked in a timely fashion.

29. Mercy did not expect Plaintiff to perform any work for Defendant gratuitously.

30. UKG operated and provided a workforce and management software, Kronos Private Cloud, by which Mercy maintained and distributed its payroll to employees.

31. UKG was acting in the interest of Mercy in relation to Plaintiff, Class Members, and all employees, by providing this workface and management software.

32. Defendants set compensation policies for Plaintiff and the Class. Defendants were jointly responsible for ensuring that Plaintiff and the Class were properly paid each pay period. Defendants were also jointly responsible for the unlawful withholding of payments subsequent to the Data Breach.

B. UKG's Data Breach.

33. Due to inadequate security measures, on or about December 11, 2021, UKG was the subject of a ransomware attack, whereby criminals obtained access to Plaintiff's and Class Members' PII and Kronos Private Cloud was rendered unusable.[3]

[3] *Id.*

34. Kronos Private Cloud is used by thousands of employers, including Mercy, and 8 million employees to manage work schedules, track hours, and calculate paychecks.[4]

35. Defendants store employees' PII in Kronos Private Cloud, which can include, *inter alia*, employee names, addresses, employee ID numbers, and social security numbers.[5]

36. The PII of millions of individuals may have been exposed to unauthorized cybercriminals when they gained access to UKG's server.[6]

37. By disclosing their PII to cybercriminals, Defendants caused Plaintiff and all Class Members not to timely receive the pay to which they were entitled and put Plaintiff and all Class Members at risk of identity theft, financial fraud, and other serious harms.

38. Defendants negligently failed to take the necessary precautions required to safeguard and protect the PII of Plaintiff and Class Members from unauthorized disclosure. Defendants' actions represent a flagrant disregard of Plaintiff's and the other Class Members' rights, both as to privacy and property.

C. Plaintiff And Class Members Were Not Paid Proper Wages.

39. Following the Data Breach, Mercy was unable to operate Kronos Private Cloud and conduct its payroll services.

40. UKG, through Kronos Private Cloud, maintained control over employee records and the rate and method of payment.

---

[4] Becky Sullivan, *Hackers disrupt payroll for thousands of employers – including hospitals*, NPR (Jan. 15, 2022), https://www.npr.org/2022/01/15/1072846933/kronos-hack-lawsuits.
[5] Jennifer Korn, *Kronos ransomware attack could impact employee paychecks and timesheets for weeks*, CNN (Dec. 17, 2021), https://www.cnn.com/2021/12/16/tech/kronos-ransomware-attack/index.html.
[6] *See id*.

41. As a result, numerous employers, including Mercy, who use Kronos Private Cloud for workforce management to manage employee schedules, track hours, and determine payment, were unable to do so.[7]

42. As a result of the Data Breach, Kronos Private Cloud was unable to function properly which restricted the rate and method of payment to employees.

43. Mercy's employees were not paid for the full amount of time they worked in one or more pay periods, or in successive pay periods, from approximately December 11, 2021 onward.

44. Plaintiff and Class Members received payment for far fewer hours than they worked.[8]

D. Plaintiff's And Class Members' Personally Identifiable Information Is Valuable.

45. PII is of great value to hackers and cyber criminals, and the data compromised in the Data Breach can be used in a variety of unlawful manners.

46. The term "personally identifiable information" refers to information that can be used to distinguish, identify, or trace an individual's identity, such as their name, Social Security number, and biometric records. This can be accomplished alone, or in combination with other personal or identifying information that is connected, or linked to an individual, such as their birthdate, birthplace, and mother's maiden name.[9]

47. Given the nature of this breach, it is foreseeable that the compromised PII can be used by hackers and cybercriminals in a variety of different ways.

---

[7] Becky Sullivan, *Hackers disrupt payroll for thousands of employers – including hospitals*, NPR (Jan. 15, 2022), https://www.npr.org/2022/01/15/1072846933/kronos-hack-lawsuits.
[8] Becky Sullivan, *Hackers disrupt payroll for thousands of employers – including hospitals*, NPR (Jan. 15, 2022), https://www.npr.org/2022/01/15/1072846933/kronos-hack-lawsuits.
[9] *See* OFFICE OF MGMT. & BUDGET, OMB MEMORANDUM M-07-16 n. 1.

48. A study by Javelin Strategy and Research found that individuals lost about $13 billion in 2020 as a result of identity fraud.[10] Data breaches and identity theft have a crippling effect on individuals and detrimentally impact the entire economy as a whole.

49. Indeed, the Social Security Administration has warned that identity thieves can use an individual's Social Security number to apply for additional credit lines.[11] Such fraud may go undetected until debt collection calls commence months, or even years, later. Stolen Social Security Numbers also make it possible for thieves to file fraudulent tax returns, file for unemployment benefits, or apply for a job using a false identity.[12] Each of these fraudulent activities is difficult to detect. An individual may not know that their Social Security Number was used to file for unemployment benefits until law enforcement notifies the individual's employer of the suspected fraud. Fraudulent tax returns are typically discovered only when an individual's authentic tax return is rejected.

50. With access to an individual's PII, cyber criminals can do more than just empty a victim's bank account -- they can also commit all manner of fraud, including: obtaining a driver's license or official identification card in the victim's name but with the thief's picture; using the victim's name and social security number to obtain government benefits; or, filing a fraudulent tax return using the victim's information. In addition, identity thieves may obtain a job using the victim's SSN, rent a house, or receive medical services in the victim's name, and may even give

[10] *See Total Identify Fraud Losses Soar to $56 Billion in 2020*, BUSINESSWIRE (Mar. 23, 2021), https://www.businesswire.com/news/home/20210323005370/en/Total-Identity-Fraud-Losses-Soar-to-56-Billion-in-2020.
[11] *Identity Theft and Your Social Security Number*, Social Security Administration (2018) at 1, https://www.ssa.gov/pubs/EN-05-10064.pdf.
[12] *Id*. at 4.

the victim's personal information to police during an arrest, resulting in an arrest warrant being issued in the victim's name.[13]

E. Defendants Were Aware of the Risk of Cyber-Attacks.

51. Data security breaches -- and data security breach litigation -- dominated the headlines in recent years, including in 2021.[14]

52. UKG's knowledge of the risks of identity theft is evidenced by its privacy notice:

> To prevent unauthorized access or disclosure, to maintain data accuracy, and to allow only the appropriate use of your [personal information], UKG utilizes physical, technical, and administrative controls and procedures to safeguard the information we collect. To protect the confidentiality, integrity, availability and resilience of your PI, we utilize a variety of physical and logical access controls, firewalls, intrusion detection/prevention systems, network and database monitoring, anti-virus, and backup systems. We use encrypted sessions when collecting or transferring sensitive data through our websites. We limit access to your PI and data to those persons who have a specific business purpose for maintaining and processing such information. Our employees who have been granted access to your PI are made aware of their responsibilities to protect the confidentiality, integrity, and availability of that information and have been provided training and instruction on how to do so.[15]

53. The cybercriminals who obtained Class Members' PII may also exploit the PII they obtained by selling the data in the so-called "dark markets." Having obtained these names,

---

[13] *See Warning Signs of Identity Theft*, FEDERAL TRADE COMMISSION, https://www.identitytheft.gov/#/Warning-Signs-of-Identity-Theft.

[14] *See e.g.*, Akanksha Rana, *T-Mobile Breach Hits 53 Million Customers as Probe Finds Wider Impact*, REUTERS (Aug. 20, 2021), https://www.reuters.com/technology/t-mobile-says-hackers-accessed-data-another-53-mln-subscribers-2021-08-20/; Jill McKeon, *St. Joseph's/Candler Suffers Ransomware Attack, EHR Downtime*, HEALTHITSECURITY (June 21, 2021), https://healthitsecurity.com/news/st-josephs-candler-suffers-ransomware-attack-ehr-downtime; David E. Sanger, Clifford Krauss, and Nicole Perlroth, *Cyberattack Forces a Shutdown of a Top U.S. Pipeline*, N.Y. TIMES (May 8, 2021), https://www.nytimes.com/2021/05/08/us/politics/cyberattack-colonial-pipeline.html.

[15] Privacy Notice, Ultimate Kronos Group, https://www.ukg.com/privacy#4243725865-507775231.

addresses, and Social Security numbers, cybercriminals can pair the data with other available information to commit a broad range of fraud in a Class Member's name.

54. In addition, if a Class Member's Social Security number is used to create a false identification for someone who commits a crime, the Class Member may become entangled in the criminal justice system, impairing the employee's ability to gain employment or obtain a loan.

F. Class Members Have Suffered Concrete Injury as a Result of Defendants' Inadequate Security and the Data Breach It Allowed.

55. Defendants represented to customers that they provided adequate security protections for their PII, and Class Members provided Defendants with sensitive personal information, including their Social Security numbers.

56. The cybercriminals will certainly use Class Members' PII, and Class Members will be at a heightened risk of identity theft for the rest of their lives. Plaintiff has incurred (and will continue to incur) damages in the form of, *inter alia*, non-payment of wages, loss of privacy and costs of protecting their credit. By this action, Plaintiff seeks to hold Defendants responsible for the harm caused by their negligence.

57. In addition, as a direct and/or proximate result of Defendants' wrongful actions and/or inaction and the resulting Data Breach, Plaintiff and Class Members have been deprived of the value of their PII, for which there is a well-established national and international market.

58. Defendants' wrongful actions and/or inaction and the resulting Data Breach have also placed Plaintiff and the other Class Members at an imminent, immediate, and continuing increased risk of identity theft and identity fraud.[16] Indeed, "[t]he level of risk is growing for

[16] *Data Breach Victims More Likely To Suffer Identity Fraud*, INSURANCE INFORMATION INSTITUTE BLOG (February 23, 2012), http://www.iii.org/insuranceindustryblog/?p=267.

anyone whose information is stolen in a data breach."[17] Javelin Strategy & Research, a leading provider of quantitative and qualitative research, notes that "[t]he theft of SSNs places consumers at a substantial risk of fraud."[18] Moreover, there is a high likelihood that significant identity fraud and/or identity theft has not yet been discovered or reported. There is also a high probability that criminals who now possess Class Members' PII have not yet used the information, but will do so at a later date or re-sell it.

59. The average cost per customer PII record was $180, based on a study by IBM and the Ponemon Institute.[19] Indeed, data breaches and identity theft have a crippling effect on individuals and detrimentally impact the entire economy as a whole.

60. As a result of the Data Breach, Plaintiff and Class Members have already suffered damages, including, but not limited to, non-payment of wages, imminent threat of identity theft, loss of privacy and the value of personal information, and deprivation of the benefit of the bargain.

61. Defendants have failed to provide adequate compensation to Class Members harmed by their negligence and for the injury caused to Plaintiff and Class Members.

CLASS ACTION ALLEGATIONS

62. Pursuant to Fed. R. Civ. P. 23, Plaintiff also brings this action against Defendants as a class action on behalf of a Class of all hourly employees of Mercy ("Mercy Class").

[17] Susan Ladika, *Study: Data Breaches Pose A Greater Risk*, CREDITCARDS.COM (July 23, 2014), http://www.creditcards.com/credit-card-news/data-breach-id-theft-risk-increase-study-1282.php.
[18] THE CONSUMER DATA INSECURITY REPORT: EXAMINING THE DATA BREACH- IDENTITY FRAUD PARADIGM IN FOUR MAJOR METROPOLITAN AREAS, http://www.nclnet.org/datainsecurity_report.
[19] *See* Abi Tyas Tunggal, *What Is The Cost of a Data Breach in 2021?*, UPGUARD (Sept. 21, 2021), https://www.upguard.com/blog/cost-of-data-breach.

63. Pursuant to Fed. R. Civ. P. 23, Plaintiff also brings this action against UKG as a class action on behalf of a Class of all individuals whose PII was compromised as a result of the Data Breach announced by UKG on or about December 11, 2021 ("National Class").

64. Plaintiff reserves the right to amend the above definition(s), or to propose other or additional classes, in subsequent pleadings and/or motions for class certification.

65. Excluded from the Class are Defendants; any parent, subsidiary, or affiliate of Defendants; any entity in which Defendants have or had a controlling interest, or which Defendants otherwise controls or controlled; and any legal representative, predecessor, successor, or assignee of Defendants.

66. This action satisfies the requirements for a class action under F.R.C.P. 23(a)(1) - (a)(4), including requirements of numerosity, commonality, typicality, and adequacy of representation.

67. This action satisfies the requirements for a class action under Rule 23(a)(1). Plaintiff believes that the proposed Class as described above consists of more than 8 million employees can be identified through Defendants' records, though the exact number and identities of Class Members are currently unknown. The Class is therefore so numerous that joinder of all members, whether otherwise required or permitted, is impracticable.

68. This action satisfies the requirements for a class action under Rule 23(a)(2). Common questions of fact and law exist for each cause of action and predominate over questions affecting only individual Class Members. Common questions include, but are not limited to, the following:

a. Whether and to what extent Defendants had a duty to protect Class Members' PII;

b. Whether Defendants breached their duty to protect Class Members' PII;

c. Whether Defendants disclosed Class Members' PII;

d. Whether Defendants' conduct was negligent;

e. Whether Plaintiff and Class Members are entitled to damages; and

f. Whether Defendants' disclosure intruded upon the privacy of Plaintiff and Class Members.

69. This action satisfies the requirements for a class action under Rule 23(a)(3). The claims asserted by Plaintiff are typical of the claims of the members of the Class she seeks to represent because, among other things, Plaintiff and Class Members sustained similar injuries as a result of Defendants' uniform wrongful conduct; Defendants owed the same duty to each class member; and Class Members' legal claims arise from the same conduct by Defendants.

70. This action satisfies the requirements for a class action under Rule 23(a)(4). Plaintiff will fairly and adequately represent and protect the interests of the Class. Plaintiff has no interests conflicting with the interests of Class Members. Plaintiff's Counsel are competent and experienced in data breach class action litigation.

71. Defendants have acted, or refused to act, on grounds generally applicable to the Class, thereby making appropriate final injunctive relief or equitable relief with respect to the Class as a whole.

72. A class action is superior to other available methods for the fair and efficient adjudication of this controversy because Class Members number in the hundreds or thousands and individual joinder is impracticable. Trial of Plaintiff's and Class Members' claims is manageable. Unless the Class is certified, Defendants will remain free to continue to engage in the wrongful conduct alleged herein without consequence.

73. The prosecution of separate actions by individual Class Members would create a risk of establishing incompatible standards of conduct for Defendants.

74. Defendants' wrongful actions, inactions, and omissions are generally applicable to the Class as a whole and, therefore, Plaintiff also seeks equitable remedies for the Class.

75. Defendants' systemic policies and practices also make injunctive relief for the Class appropriate.

76. Absent a class action, Defendants will retain the benefits of its wrongdoing despite its serious violations of the law and infliction of economic damages, injury, and harm on Plaintiffs and Class Members.

CAUSES OF ACTION

FIRST CAUSE OF ACTION
Against Mercy Defendants On Behalf Of Plaintiff And The Mercy Class
(Violation Of The Massachusetts Wage Act)

77. Plaintiff re-alleges and incorporates by reference all preceding factual allegations as though fully set forth herein.

78. Mercy has been and continues to be an "employer" of Plaintiff and the Mercy Class within the meaning of the Massachusetts Wage Act (M.G.L. c. 149).

79. Plaintiff and the Mercy Class Members were "employees" of Mercy within the meaning of Massachusetts Wage Act (M.G.L. c. 149).

80. Mercy employed Plaintiff and the Mercy Class Members, suffering or permitting them to work within the meaning of Massachusetts Wage Act (M.G.L. c. 149).

81. Mercy failed to pay regular wages owed to Plaintiff and the Mercy Class Members on a timely basis for the work which they did for Mercy, and that Mercy did so willfully, in violation of the Massachusetts Wage Act (M.G.L. c. 149).

82. As the result of the Mercy's violations of Massachusetts law set forth above, Plaintiff and the Mercy Class Members have incurred damages in an amount to be determined at trial, along with liquidated damages, attorneys' fees and costs of litigation.

83. All prerequisites and conditions precedent necessary to seek the remedies sought in this action have been satisfied, including the administrative notice requirement to the Massachusetts Attorney General.

SECOND CAUSE OF ACTION
Against All Defendants On Behalf of The Mercy Class
And Against UKG On Behalf Of The National Class
(Negligence)

84. Plaintiff re-alleges and incorporates by reference all preceding factual allegations as though fully set forth herein.

85. Defendants owed a duty to Plaintiff and to the Class to exercise reasonable care in obtaining, securing, safeguarding, properly disposing of and protecting Plaintiffs and Class Members' sensitive information within its control from being compromised by or being accessed by unauthorized third parties. This duty included, among other things, maintaining adequate control over its computer systems and network so as to prevent unauthorized access thereof.

86. Defendants had full knowledge of the sensitivity of PII and the types of harm that Plaintiff and Class Members could and would suffer if the PII were compromised.

87. Defendants had a duty to exercise reasonable care to avoid foreseeable harm in its retention of Plaintiff's and Class Member's PII.

88. Defendants owed a duty of care to Plaintiff and members of the Class to provide security, consistent with industry standards, to ensure that its computer systems adequately protected the sensitive information of the patients in its facilities and networks.

89. Defendants breached their duty of care by failing to secure and safeguard the PII of

Plaintiff and Class Members. Defendants failed to use reasonable measures to protect Class Members' PII. Defendants negligently stored and/or maintained its servers and systems.

90. It was foreseeable that Defendants' failure to use reasonable measures to protect Plaintiff's and Class Members' PII would result in injury to Plaintiff and other Class Members. Further, the breach of security, unauthorized access, and resulting injury to Plaintiff and Class Members were reasonably foreseeable.

91. It was foreseeable that Defendants knew or should have known that its failure to exercise adequate care in safeguarding and protecting Plaintiff's and Class Members' PII would result in its release and disclosure to unauthorized third parties who, in turn, wrongfully used such PII or disseminated it for wrongful use.

92. Therefore, it was foreseeable to Defendants that the failure to adequately safeguard PII would result in one or more of the following injuries to Plaintiff and Class Members: an imminent threat of identity theft, delay or error in payment of wages, necessary mitigation expenses, loss of privacy and the value of personal information, deprivation of the benefit of the bargain, ongoing and imminent impending threat of identity theft crimes, fraud and abuse, resulting in monetary loss and economic harm; actual identity theft crimes, fraud, and abuse, resulting in monetary loss and economic harm; loss of confidentiality of the stolen confidential data; expenses and/or time spent on credit monitoring and identity theft insurance; time spent scrutinizing bank statements, credit card statements, and credit reports; expenses and/or time spent initiating fraud alerts, decreased credit scores and ratings; and other economic and non-economic harm.

93. But for Defendants' negligent and wrongful breach of its responsibilities and duties owed to Plaintiff and Class Members, the PII of Plaintiff and Class Members would not have been

compromised.

94. Had Defendants not failed to implement and maintain adequate security measures to protect the PII of its employees, Plaintiff's and Class Members' PII would not have been exposed to unauthorized access and they would not have suffered any harm.

95. As a direct and proximate result of Defendants' above-described wrongful actions, inactions, and omissions, the resulting Data Breach, and the unauthorized release and disclosure of PII, Plaintiff and Class Members have incurred, and will continue to incur, the above-referenced damages, and other actual injury and harm.

96. Defendants' wrongful actions, inactions, and omissions constituted (and continues to constitute) common law negligence.

97. Plaintiff and the Class seek damages, injunctive relief, and other and further relief as the Court may deem just and proper.

THIRD CAUSE OF ACTION
Against All Defendants On Behalf of The Mercy Class
And Against UKG On Behalf Of The National Class
(Intrusion Upon Seclusion/Invasion Of Privacy)

98. Plaintiff re-alleges and incorporates by reference all paragraphs above as if fully set forth herein.

99. The State of Massachusetts recognizes the right against "unreasonable, substantial or serious interference" with an individual's privacy. M.G.L.A. 214 § 1B.

100. Plaintiff and the Class Members had a reasonable expectation of privacy in the PII Defendants mishandled.

101. By intentionally failing to keep Plaintiff's and the Class Members' PII safe, and by intentionally misusing and/or disclosing said information to unauthorized parties for unauthorized use, Defendants intentionally invaded Plaintiffs' and Class Members' privacy by intrusion.

102. Defendants knew that ordinary persons in Plaintiff's or the Class Members' positions would consider this an invasion of privacy and Defendants' intentional actions highly offensive and objectionable.

103. Defendants invaded Plaintiff's and the Class Members' right to privacy and intruded into Plaintiff's and the Class Members' private affairs by intentionally misusing and/or disclosing their PII without their informed, voluntary, affirmative, and clear consent.

104. In failing to protect Plaintiff's and the Class Members' PII, and in intentionally misusing and/or disclosing their PII, Defendants acted with intentional malice and oppression and in conscious disregard of Plaintiff's and the Class Members' rights to have such information kept confidential and private.

105. Plaintiff and the Class Members sustained damages (as outlined above) as a direct and proximate consequence of the invasion of their privacy by intrusion, and therefore seek an award of damages.

FOURTH CAUSE OF ACTION
Against All Defendants On Behalf of The Mercy Class
And Against UKG On Behalf Of The National Class
(Breach of Fiduciary Duty)

106. Plaintiff re-alleges and incorporates by reference all paragraphs above as if fully set forth herein.

107. In providing their PII to Defendants, Plaintiff and Class Members justifiably placed special confidence in Defendants to act in good faith and with due regard to the interests of Plaintiff and Class Members in order to safeguard and keep confidential their PII.

108. Defendants accepted the special confidence placed in it by Plaintiff and Class Members, as evidenced by its assertion stated above in their privacy notices and policies. There was an understanding between the parties that Defendants would act for the benefit of Plaintiff and

Class Members in preserving the confidentiality of the PII.

109. In light of the special relationship between Defendants, Plaintiff, and the Class Members, whereby Defendants became the guardian of Plaintiff's and the Class Members' PII, Defendants accepted a fiduciary duty to act primarily for the benefit of its employees, including Plaintiff and the Class Members. This duty included safeguarding Plaintiff's and the Class Members' PII.

110. Defendants have a fiduciary duty to act for the benefit of Plaintiff and Class Members upon matters within the scope of its employment relationship with its employees, in particular, to keep secure the PII of those employees.

111. Defendants breached their fiduciary duties to Plaintiff and the Class Members by failing to encrypt and otherwise protect the integrity of its computer systems containing Plaintiff's and the Class Members' PII.

112. Defendants breached the fiduciary duties they owed to Plaintiff and the Class Members by failing to timely notify and/or warn them of the Data Breach.

113. Defendants breached their fiduciary duties by failing to ensure the confidentiality and integrity of electronic PII Defendant created, received, maintained, and transmitted.

114. Defendants breached their fiduciary duties by failing to implement technical policies and procedures for electronic information systems that maintain electronic PII to allow access only to those persons or software programs that have been granted access rights.

115. Defendants breached their fiduciary duties by failing to implement policies and procedures to prevent, detect, contain, and correct security violations.

116. Defendants breached their fiduciary duties by failing to identify and respond to suspected or known security incidents and to mitigate, to the extent practicable, harmful effects of

security incidents that are known to the covered entity.

117. Defendants breached their fiduciary duties by impermissibly and improperly using and disclosing PII that is and remains accessible to unauthorized persons.

118. Defendants breached their fiduciary duties by failing to design, implement, and enforce policies and procedures establishing physical and administrative safeguards to reasonably safeguard PII.

119. Defendants breached their fiduciary duties by otherwise failing to safeguard Plaintiff's and the Class Members' Private Information.

120. As a direct and proximate result of Defendants' breaches of their fiduciary duties, Plaintiff and Class Members have suffered and will suffer injury, including but not limited to: (i) actual identity theft; (ii) the compromise, publication, and/or theft of their PII; (iii) out-of-pocket expenses associated with the prevention, detection, and recovery from identity theft and/or unauthorized use of their Private Information; (iv) lost opportunity costs associated with effort expended and the loss of productivity addressing and attempting to mitigate the actual and future consequences of the Data Breach, including but not limited to efforts spent researching how to prevent, detect, contest, and recover from identity theft; (v) the continued risk to their PII, which remains in Defendants' possession and is subject to further unauthorized disclosures so long as Defendants fail to undertake appropriate and adequate measures to protect the Private Information in its continued possession; and (vi) future costs in terms of time, effort, and money that will be expended as result of the Data Breach for the remainder of the lives of Plaintiffs and Class Members.

121. As a direct and proximate result of Defendants' breaches of their fiduciary duties, Plaintiff and Class Members have suffered and will continue to suffer other forms of injury and/or

harm, and other economic and non-economic losses.

FIFTH CAUSE OF ACTION
Against All Defendants On Behalf of The Mercy Class
And Against UKG On Behalf Of The National Class
(Declaratory and Injunctive Relief)

122. Plaintiff re-alleges and incorporates by reference all paragraphs above as if fully set forth herein.

123. This Count is brought under the federal Declaratory Judgment Act, 28 U.S.C. §2201.

124. Defendants owe a duty of care to Plaintiff and Class Members requiring it to adequately secure their PII.

125. Defendants still possesses Plaintiff's and Class Members' PII.

126. Since the Data Breach, Defendants have announced few, if any, changes to its data security infrastructure, processes, or procedures to fix the vulnerabilities in its computer systems and/or security practices which permitted the Data Breach to occur and, thereby, prevent future attacks.

127. Defendants have not satisfied legal duties to Plaintiff and Class Members. In fact, now that Defendants' insufficient data security is known to hackers, the PII in Defendants' possession is even more vulnerable to cyberattack.

128. Actual harm has arisen in the wake of the Data Breach regarding Defendants' duties of care to provide security measures to Plaintiff and Class Members. Further, Plaintiff and Class Members are at risk of additional or further harm due to the exposure of their PII and Defendants' failure to address the security failings that led to such exposure.

129. There is no reason to believe that Defendants' security measures are any more adequate now than they were before the Data Breach to meet Defendant's legal duties.

130. Plaintiff, therefore, seeks a declaration (1) that Defendants' existing security measures do not comply with its duties of care to provide adequate security, and (2) that to comply with its duties of care, Defendants must implement and maintain reasonable security measures, including, but not limited to:

a. Ordering that Defendants engage third-party security auditors/penetration testers as well as internal security personnel to conduct testing, including simulated attacks, penetration tests, and audits on Defendants' systems on a periodic basis, and ordering Defendants to promptly correct any problems or issues detected by such third-party security auditors;

b. Ordering that Defendants engage third-party security auditors and internal personnel to run automated security monitoring;

c. Ordering that Defendants audit, test, and train its security personnel regarding any new or modified procedures;

d. Ordering that Defendants segment data by, among other things, creating firewalls and access controls so that if one area of Defendants' systems is compromised, hackers cannot gain access to other portions of Defendants' systems;

e. Ordering that Defendants purge, delete, and destroy in a reasonably secure manner customer data not necessary for its provisions of services;

f. Ordering that Defendants conduct regular computer system scanning and security checks;

g. Ordering that Defendants routinely and continually conduct internal training and education to inform internal security personnel how to identify and contain a breach when it occurs and what to do in response to a breach; and

h. Ordering Defendants to meaningfully educate its current, former, and prospective customers about the threats they face as a result of the loss of their PII to third parties, as well as the steps they must take to protect themselves.

PRAYER FOR RELIEF

WHEREFORE, Plaintiff, on behalf of herself and the Class, respectfully request that the Court grant relief against Defendant as follows:

A. Certifying this class action pursuant to Rule 23 of the Federal Rules of Civil Procedure and requiring notice thereto to be paid by Defendants;

B. Appointing Plaintiff and her counsel to represent the Class;

C. For appropriate injunctive relief and/or declaratory relief, including an Order requiring Defendants to immediately secure and fully encrypt all confidential information, to properly secure computers containing confidential information, to cease negligently storing, handling, and securing its Employees' confidential information, and to provide identity theft monitoring for an additional five years;

D. Adjudging and decreeing that Defendants have engaged in the conduct alleged herein;

E. For compensatory and general damages according to proof on certain causes of action;

F. For reimbursement, restitution, and disgorgement on certain causes of action;

G. For both pre- and post-judgment interest at the maximum allowable rate on any amounts awarded;

H. For costs of the proceedings herein;

I. For an Order awarding Plaintiff and the Class reasonable attorney's fees and expenses for the costs of this suit;

J. Trial by jury; and

K. For any and all such other and further relief that this Court may deem just and proper, including but not limited to punitive or exemplary damages.

Dated: July 20, 2022

Respectfully Submitted,

For Plaintiff and Class Members,

By their attorneys:

FINKELSTEIN, BLANKINSHIP, FREI-PEARSON & GARBER, LLP

By: */s/ D. Greg Blankinship*
D. Greg Blankinship (BBO #655430)
Jeremiah Frei-Pearson (*pro hac vice* application forthcoming)
One North Broadway, Suite 900
White Plains, New York 10601
Tel.: (914) 298-3281
gblankinship@fbfglaw.com
jfrei-pearson@fbfglaw.com

Jack J. Canzoneri (BBO #564126)
Nicholas Wanger (BBO #PENDING)
MCDONALD LAMOND CANZONERI
352 Turnpike Rd., Suite 210
Southborough, MA 01772
Tel.: (508) 485-6600
jcanzoneri@masslaborlawyers.com
nwanger@masslaborlawyers.com

Attorneys for Plaintiff and the Proposed Classes